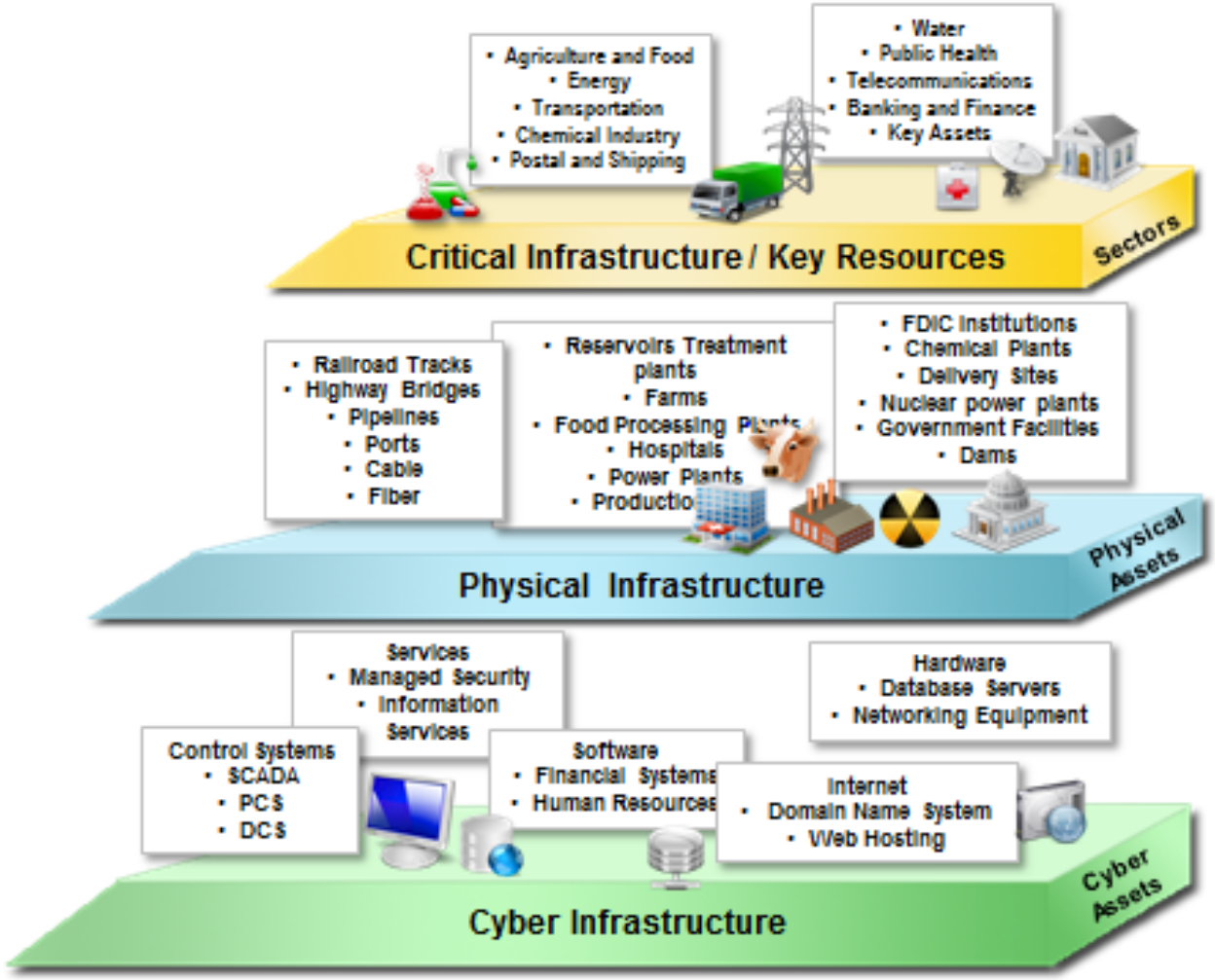
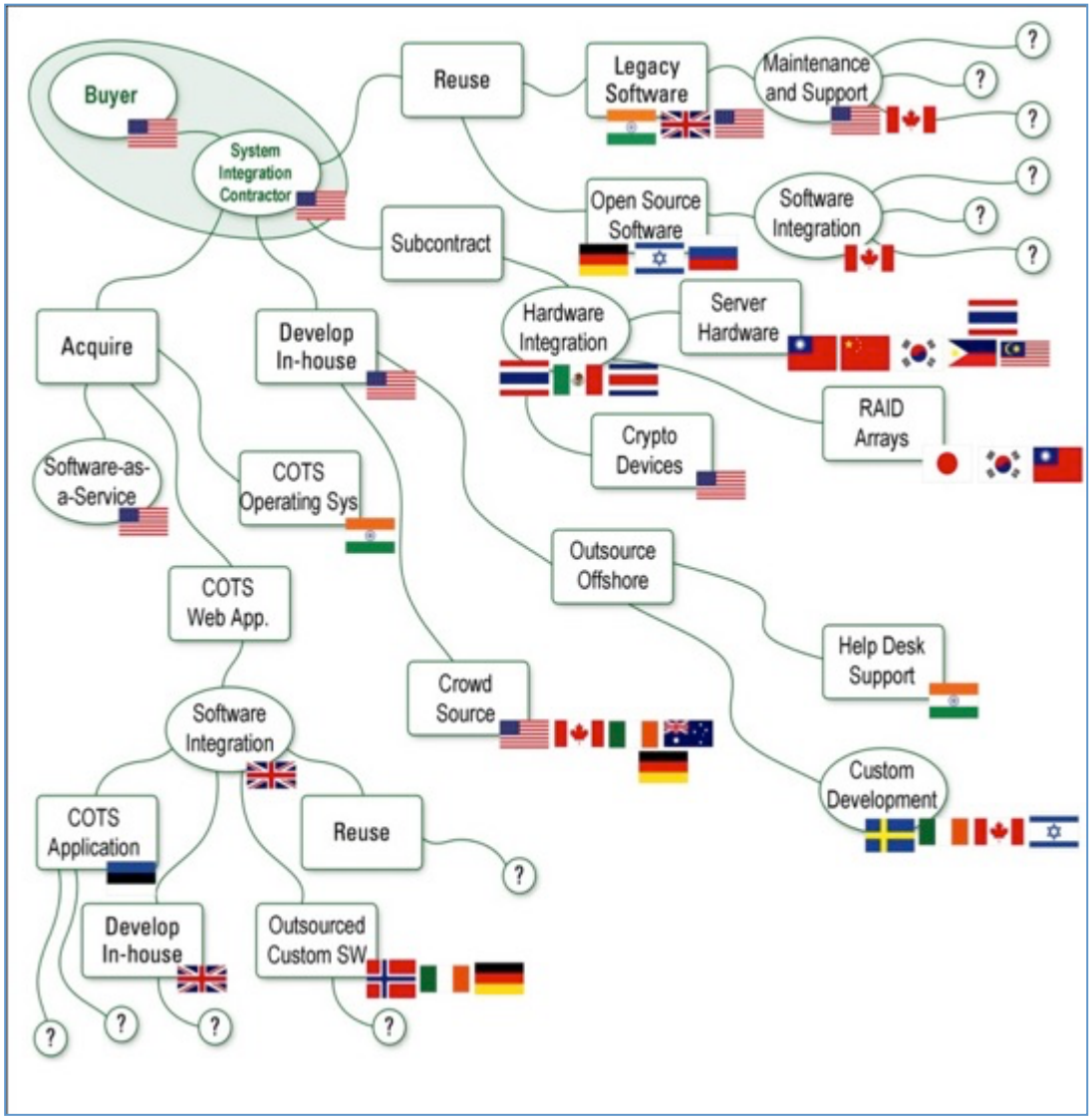
Evolutions in SSCA Best Practice Adoption
SSCA Fall Forum 2015

Our Technology Enabled Environment



A Simplified ICT Supply Chain



Challenges With Technology

Vulnerability

- A *(software) vulnerability* is a collection of one or more weaknesses that contain the right conditions to permit unauthorized parties to force the software to perform unintended behavior (a.k.a. "is exploitable")
- CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.

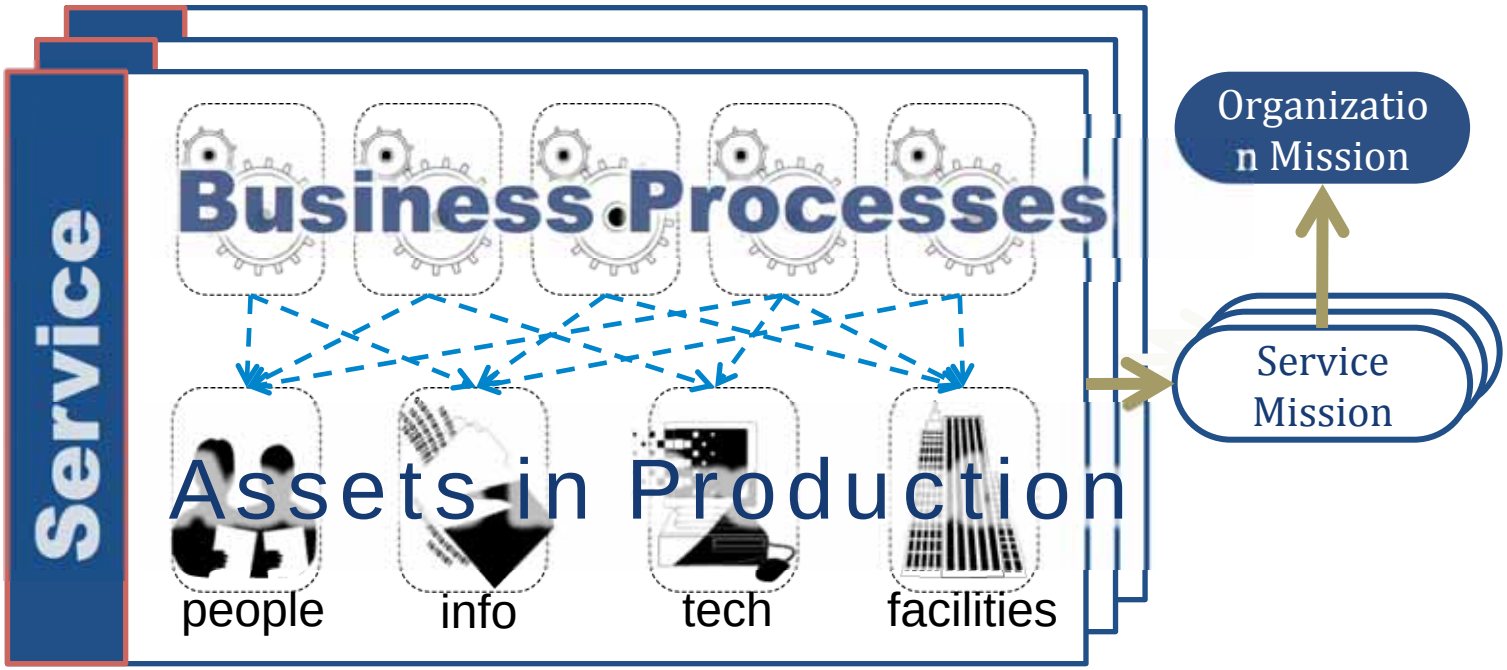
Weakness

- A *(software) weakness* is a property of software/systems that, under the right conditions, may permit unintended / unauthorized behavior.

- The Common Weakness Enumeration (CWE™) is a list of software weaknesses.

Source: http://makingsecuritymeasurable.mitre.org/ and DHS Software Assurance Program

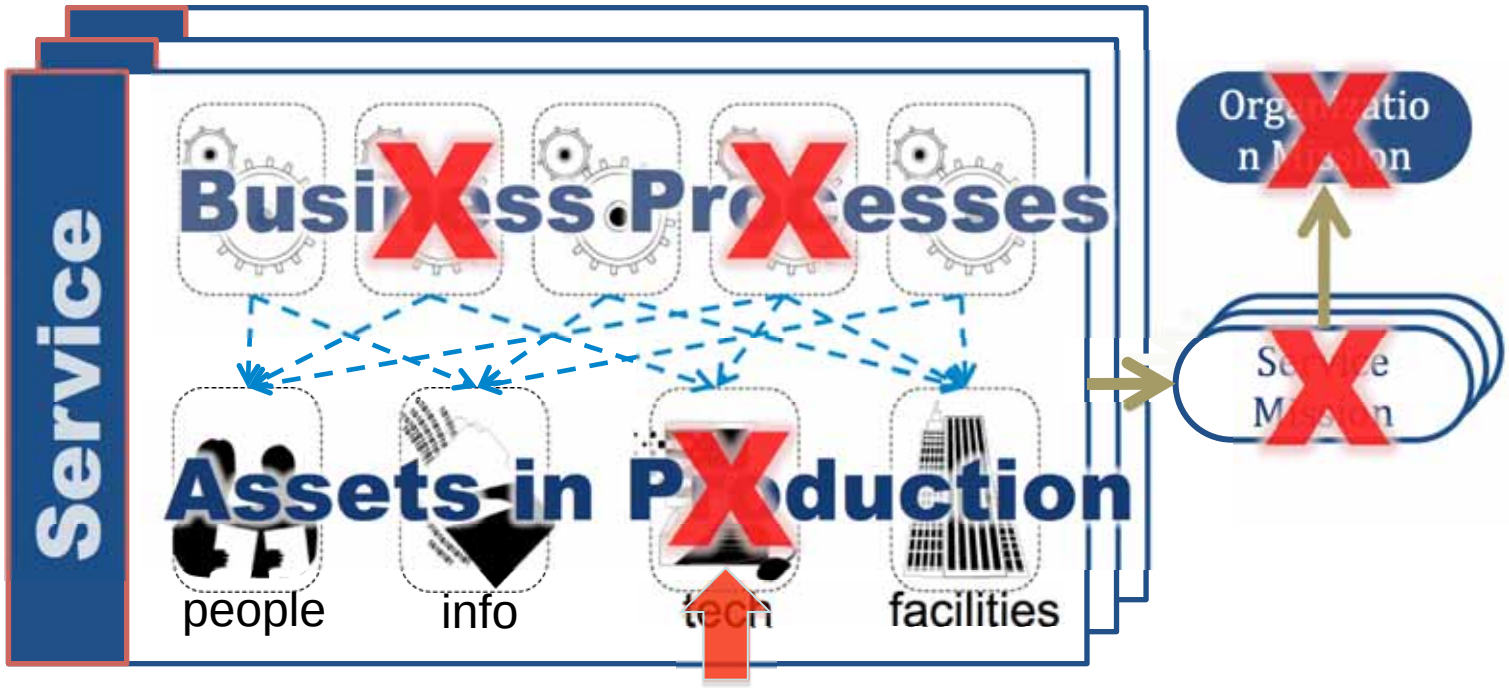
Reliable Technology



CERT | Software Engineering Institute | Carnegie Mellon.

Adapted from: November 2009 SwA Forum-Evolution in SwA Processes Panel – David White, SEI

Defect and/or Exploited Vulnerability In Operations



CERT | Software Engineering Institute | Carnegie Mellon.

Adapted from: November 2009 SwA Forum-Evolution in SwA Processes Panel – David White, SEI

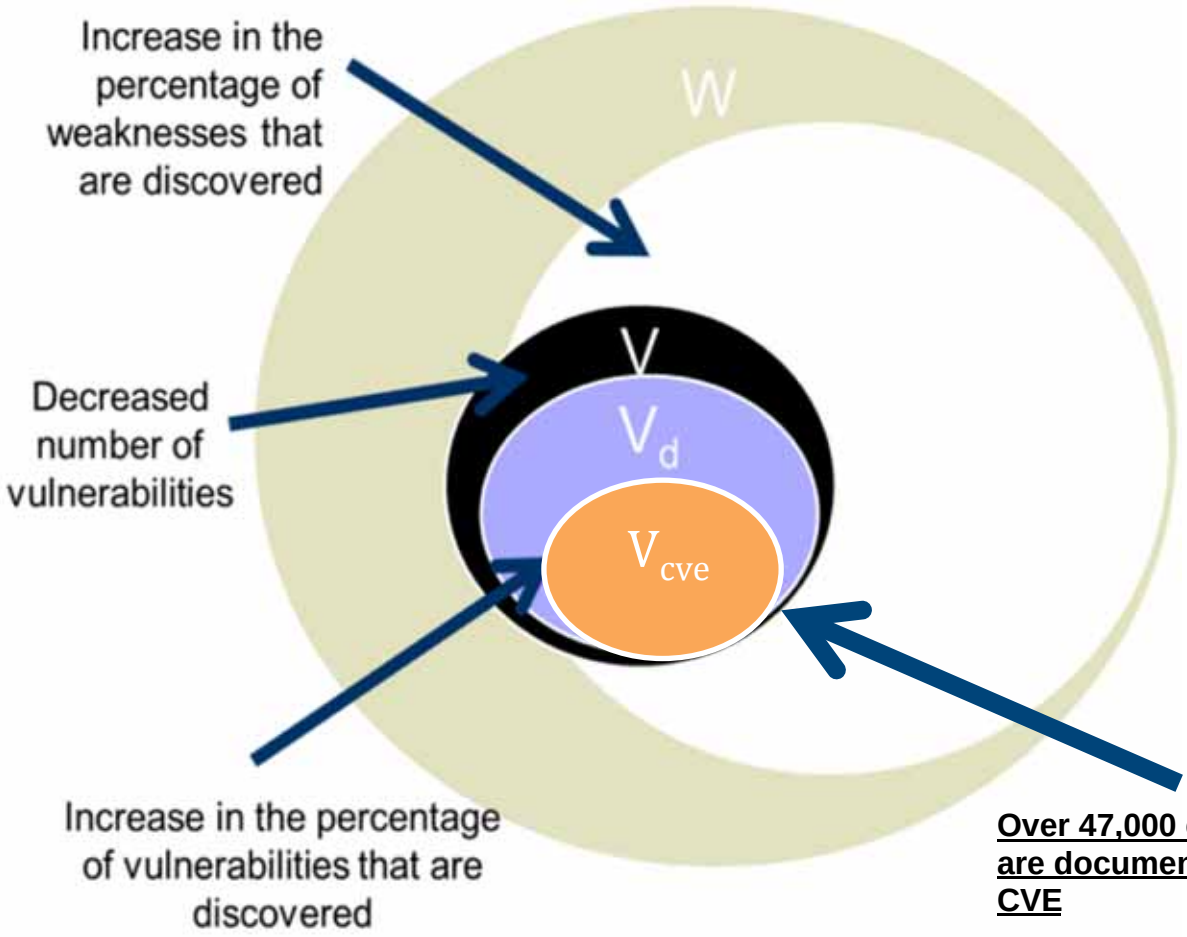
Asset Management Need Identified in 2011 Cyber Studies

- Often Ignored Security Practices
  - **Know your assets and manage access to them, and their configurations and vulnerabilities**
  - Risk assessment
  - **Manage data assets**
  - Maintain audit logs and analyze them
  - Plan for and know that you are prepared for an incident or disaster
  - **Secure design, coding, integration, and test**
  - Ensure repeatable business processes
  - Training and awareness

Additional information on the value of these essential security practices can be found in the

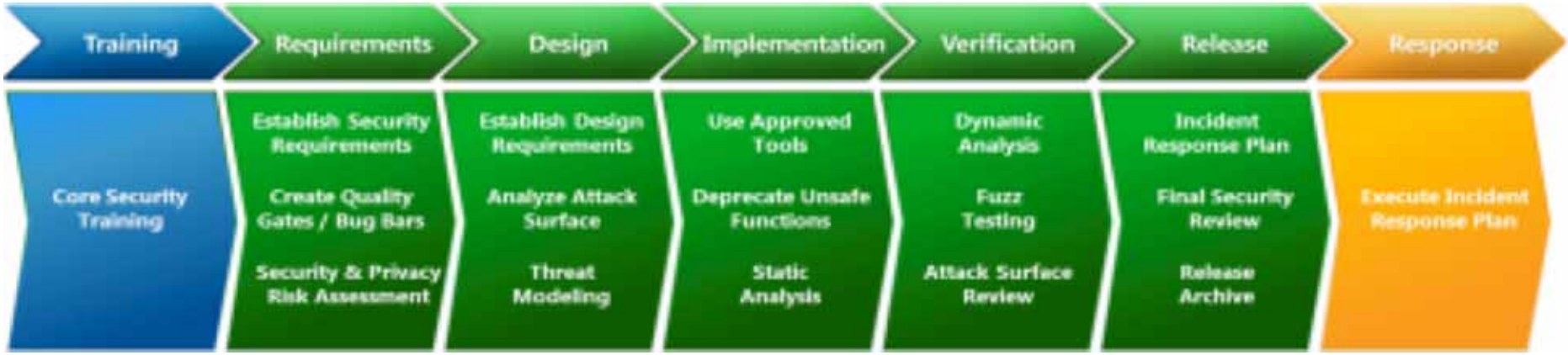
- 2011 Verizon Data Breach Investigations Report
- Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011
- NIST Interagency Report 7622 - Piloting Supply Chain Risk. Management for Federal Information Systems

Vulnerabilities In Technology Assets Are Tracked

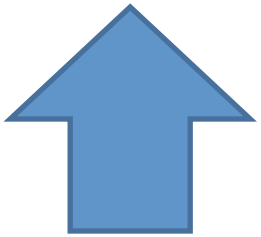


Adapted from Richard Struse, DHS Software Assurance Program

Processes Exist for Reporting and Patching Vulnerabilities



Microsoft Secure Development Lifecycle



Unpatched Vulnerabilities Are Known Attack Targets

- 99.9% OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED

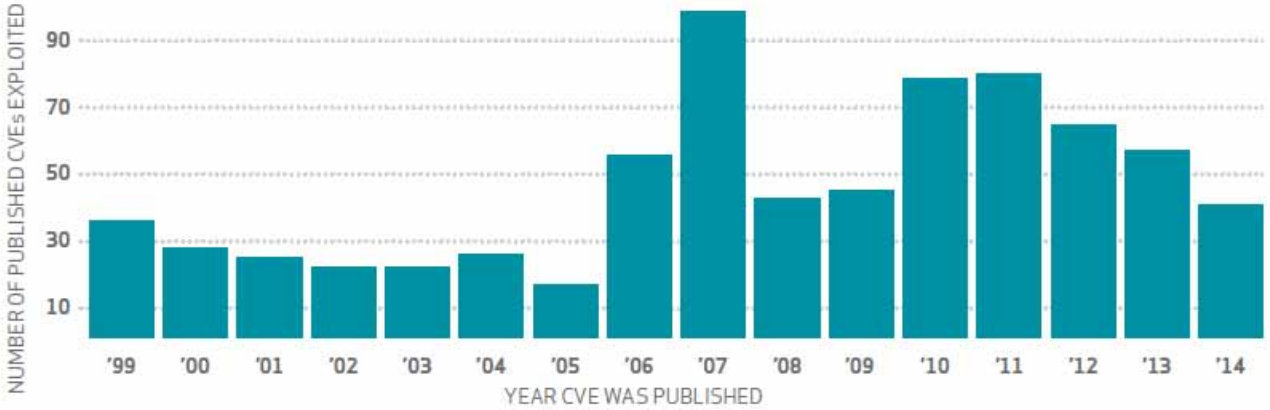


Figure 10.

Count of exploited CVEs in 2014 by CVE publish date

Asset Management Increases Cost for Attackers

Tripwire survey of 215 attendees at the Black Hat USA 2015

- 64% of organizations believe themselves to be potential targets for nation-state cyberattacks
- 86% of the respondents also said they have seen an increase in targeted attacks directed at their networks over the past year.

Tripwire's Tim Erlin recommends small businesses ensure they have basic foundational controls before worrying about the latest 'sophisticated' attack, as **"simply keeping systems on current software, effectively patching vulnerabilities,** and ensuring critical systems are running hardened configurations can significantly **increase the cost to the attacker.“**

Businesses See Sharp Rise in Targeted Attack *eWeek (08/17/15) Eddy, Nathan*

Software Identification Tags

NIST

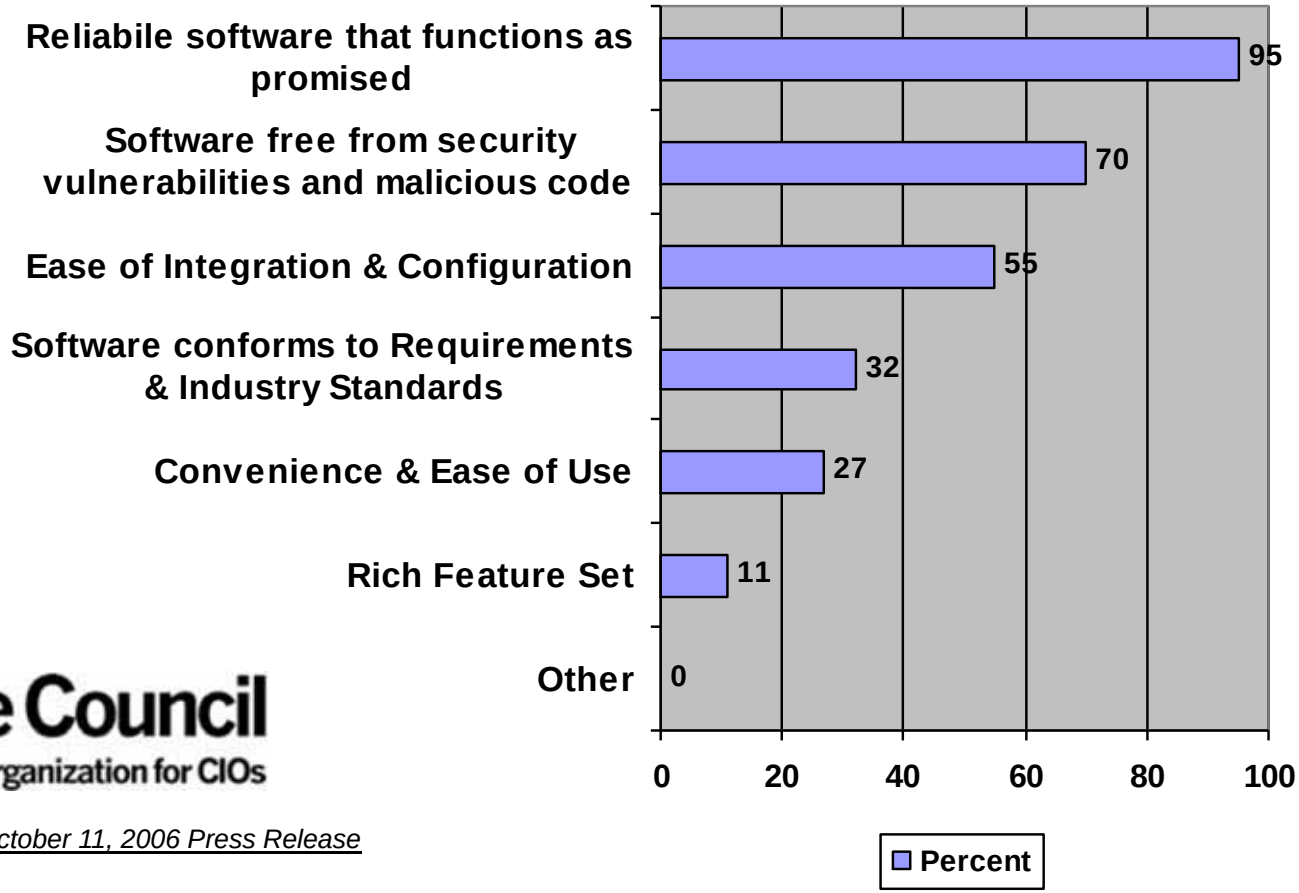
- **NIST's Computer Security Division released the third Draft NIST Interagency Report (NISTIR) 8060, Guidelines for the Creation of Interoperable Software Identification (SWID) Tags is available for public comment.** http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8060
- **Deadline to submit comments: September 24, 2015.**

ISO

- SAM/ITAM process standard ISO/IEC 19770-1 update effort
- Participation from SC27 (Information security) is particularly requested because of the strong interdependence of security and IT asset management.

CIOs Wanted Secure Software

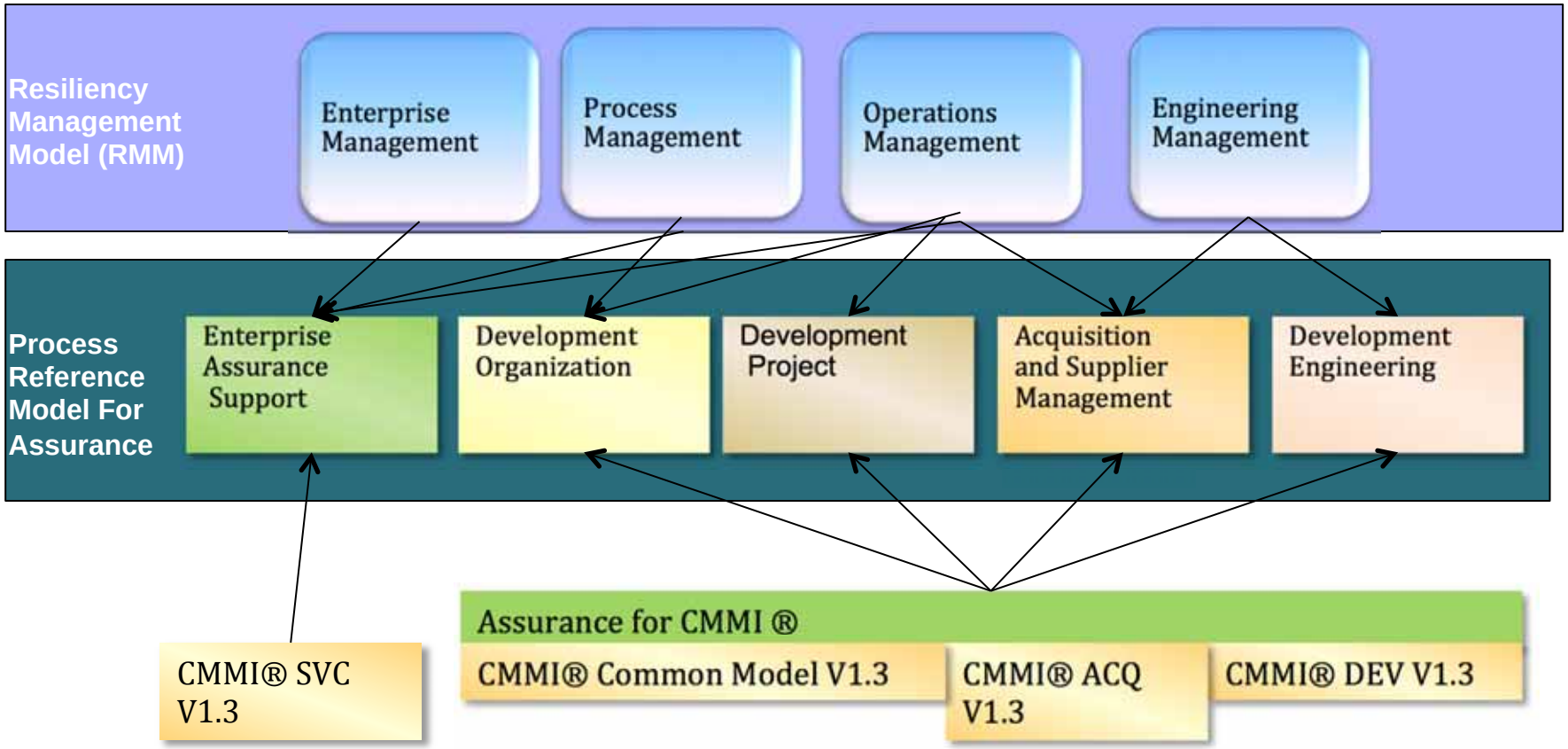
What CIOs want



CIO Executive Council
The Professional Organization for CIOs

https://www.cioexecutivecouncil.com October 11, 2006 Press Release

Efforts to Communicate to Executives



https://buildsecurityin.us-cert.gov/swa/proself_assm.html

Assurance Process Reference Model

Define Business Goals

Development Project

DP 1 Identify and manage risks due to vulnerabilities throughout the product and system lifecycle

DP 2 Establish and maintain assurance support from the project

DP 3 Protect project and organizational assets

Enterprise Assurance Support

ES 1 Establish and maintain organizational culture where assurance is an integral part of achieving the mission

ES 2 Establish and maintain the ability to support continued delivery of assurance capabilities

ES 3 Monitor and improve enterprise support to IT assets

Development Organization

DO 1 Establish the assurance resources to achieve key business objectives

DO 2 Establish the environment to sustain the assurance program within the organization

Prioritize funds and manage risks

Acquisition and Supplier Management

AM 1 Select, manage, and use effective suppliers and third party applications based upon their assurance capabilities.

Development Engineering

DE 1 Establish assurance requirements

DE 2 Create IT solutions with integrated business objectives and assurance

DE 3 Verify and Validate an implementation for assurance

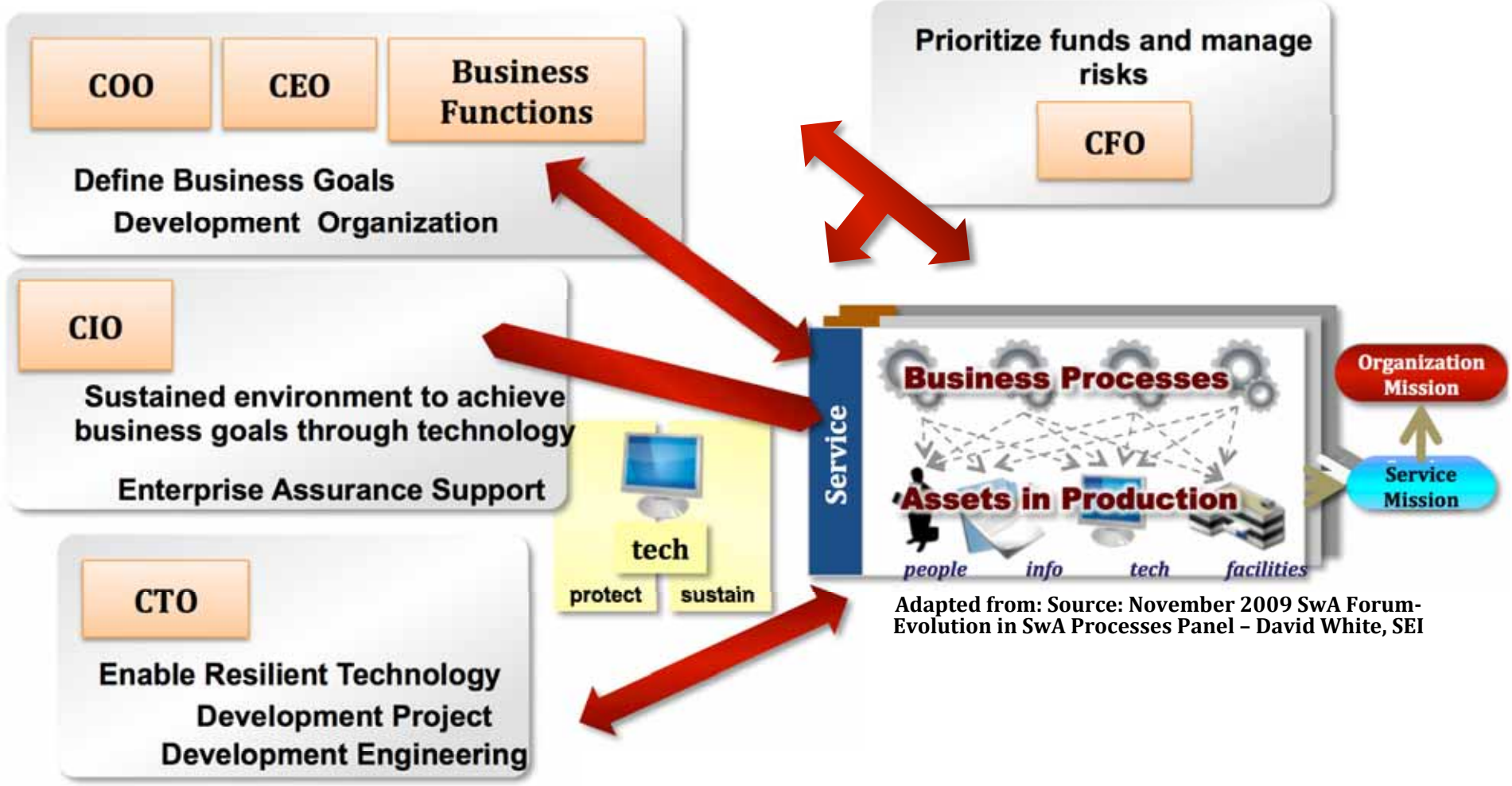
Enable Resilient Technology

Sustained environment to achieve business goals through technology

The Assurance PRM Is A Holistic Framework that connects CMMI and RMM to facilitate communication

https://buildsecurityin.us-cert.gov/swa/proself_assm.html

Efforts to Communicate To Executives Continue



Adapted from: Source: November 2009 SwA Forum- Evolution in SwA Processes Panel – David White, SEI

Learning From Success Stories

- **Who**
  - Specialists (i.e. SwA SMEs)
  - Practitioners (Developers)
- **What**
  - Measure progress
  - Internal policy
- **When**
  - During product development process
  - During Leadership discussions
  - As part of development and acquisition reviews
- **Where**
  - IT Development Organizations
  - IT Acquisition Organizations
  - IT Integrator Organizations

- **Why**
  - Customer pressure
  - Reaction to an incident
- **Why Not**
  - Software security is not an explicit requirement in development contracts or acquisition processes
  - Secure software training is not given to developers and architects
- **How**
  - **Executive leadership commitment**
  - Translate ROI to project manager vocabulary (cost, schedule, quality)
  - Start small and build
  - Use standards (i.e. coding standards)
  - Avoid creating a new language
  - Leverage what is already known
  - Increase automation of menial tasks

Courtesy of September 2010 SwA Panel SwA Practices – Getting to Effectiveness in Implementation

The Need to Address Code Vulnerabilities Still Overlooked

- Ernst and Young –SwA is not a top technology driver – the need for Software Assurance is overtaken by the need for mobile workforce, cloud computing, social networking
  - 60% perceive an **increase in risk** due to social networking, cloud computing and personal devices in the enterprise
  - 46% indicated that their investment in information security is **increasing** over last year
  - 53% indicated that workforce mobility is a **significant challenge to information security**
  - 64% indicated that disclosure of sensitive data was one of **top five areas of IT risk**
  - 50% plan on spending more over the next year on data leakage/data loss prevention
  - 23% currently employing cloud computing, with 77% of those using Software as a Service model

Include software related risks in discussions about leadership priorities

Understanding Trends in SwA Adoption June 28, 2011

Are We Making Progress?

- 11 % of public company boards reported a high level understanding of cybersecurity (According to A National Association of Corporate Directors Report)
- 30 % of boards do not even talk about cybersecurity (a PricewaterhouseCoopers study)

Companies With Computer-security Knowledgeable Board Members

AIG, Blackberry, Parsons Corp., CMS Energy, General Motors, and Wells Fargo

Source: Companies Hope Cybersecurity Experts in the Boardroom Can Counter Hacks: *Los Angeles Times (08/17/15) Dave, Paresh*

Reaching the C-Level

- Charlie Tupitza, Axelos